# Susan S Bies: Strengthening compliance through effective corporate governance

Remarks by Ms Susan S Bies, member of the Board of Governors of the US Federal Reserve System, at the American Bankers Association, Annual Regulatory Compliance Conference in Washington DC, 11 June 2003.

* * *

Good morning. I thank you for the invitation to speak to this American Bankers Association Regulatory Compliance Conference. Since coming to the Federal Reserve Board, I have spent much of my time dealing with corporate governance, internal control, and risk management issues. Today, I would like to talk with you about the important role that the compliance function plays in banking organizations, and how the current emphasis on improving corporate governance is an opportunity for you to strengthen the compliance function in your organization.

## Introduction

Over the past two years, we all have been shocked by the headlines announcing corporate governance or accounting problems at a variety of companies, such as Enron, Worldcom, and HealthSouth. As we read these headlines, the question that comes to mind is, "What were the underlying deficiencies in the internal control processes of these companies that rendered their governance practices ineffective?" As the details about the scandals have been made public, it has become clear that they exemplify breakdowns in fundamental systems of internal control. Why, then, have we seen so many headlines highlighting corporate governance and accounting problems? Because these companies lost track of the basics of effective corporate governance - internal controls and a strong ethical compass. While most companies have effective governance processes in place, these events remind all of us of the importance of doing the basics well.

## Internal control framework

After an earlier series of corporate frauds, the National Commission on Fraudulent Financial Reporting, also known as the Treadway Commission, was created in 1985 to make recommendations to reduce the incidence of these types of frauds. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission issued a report titled *Internal Control - Integrated Framework* that has become the most-referenced standard on internal control.

If one re-reads that report, the need to return to focusing on the basics becomes clear. The report defines internal control as:

*a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of...*

- Effectiveness and efficiency of operations
- Reliability *of financial reporting*
- Compliance *with applicable laws and regulations.*

The COSO framework was the model considered when the Federal Deposit Insurance Corporation Improvement Act (FDICIA) was enacted in 1991. Section 112 of FDICIA requires management to report annually on the quality of internal controls and outside auditors to attest to that control evaluation.

## Control assessments

COSO requires all managers to, at least once a year, step back from their other duties and evaluate risks and controls within their span of authority. Each manager should consider current and planned

operational changes, identify risks, determine appropriate mitigating controls, establish an effective monitoring process, and evaluate the effectiveness of those controls. Managers then should report their assessment up the chain of command to the chief executive officer, with each new level of management in turn considering the risks and controls under its responsibility. The results of this process are ultimately reported to the audit committee of the board of directors. In the case of banks, management publicly reports on its assessment of the effectiveness of controls over financial reporting and the external auditor is required to attest to this self-assessment. Thus, the process helps managers communicate among themselves and with the board about the dynamic issues affecting risk exposures, risk appetites, and risk controls throughout the company.

Risk assessments such as the one outlined in COSO presumably could also be useful in assessing various lines of business when formulating business strategies. But not all corporations and boards consider risk during their annual strategic planning or other evaluation processes. The 2002 survey of corporate directors conducted jointly by the Institute of Internal Auditors and the National Association of Corporate Directors showed that directors are not focusing on risk management. I was surprised to learn that 45 percent of directors surveyed said their organization did not have a formal enterprise risk-management process - or any other formal method of identifying risk. An additional 19 percent said they were not sure whether their company had a formal process for identifying risks. These percentages indicate that some companies have directors who don't understand their responsibilities as the representatives of shareholders. The shareholders of those companies should be asking the directors how they govern an organization without a good understanding of the risks the company is facing and without knowledge of a systematic approach to identifying, assessing, monitoring, and mitigating excessive risk-taking. I trust that none of the directors who participated in the survey were on the board of a financial services company.

Although directors are not expected to understand every nuance of every line of business or to oversee every transaction, they do have responsibility for setting the tone regarding their corporations' risk-taking and establishing an effective monitoring program. They also have responsibility for overseeing the internal control processes, so that they can reasonably expect that their directives will be followed. They are responsible for hiring individuals who have integrity and can exercise sound judgment and are competent. In light of recent events, I might add that directors have a further responsibility for periodically determining whether their initial assessment of management's integrity was correct.

The COSO framework and FDICIA annual report can be an effective tool for the auditor to communicate risks and control processes to the audit committee. Members of that committee should use the reports to be sure business strategy, changing business processes, management reorganizations, and positioning for future growth are conducted within the context of a sound system of internal controls and governance. The report should identify priorities for strengthening the effectiveness of internal controls.

Indeed, beyond legal requirements, boards of directors of all firms should periodically assess where management, which has stewardship over shareholder resources, stands on ethical business practices. They should ask, for example: "Are we getting by on technicalities, adhering to the letter but not the spirit of the law? Are we compensating ourselves and others on the basis of contribution, or are we taking advantage of our positions? Would our reputation be tainted if word of our actions became public?" Compliance officers should help ensure that processes are in place for employees to raise ethical and compliance concerns in an environment that protects them from retribution from affected managers.

**Internal controls over compliance**

Risk management clearly cannot be effective within a company if we forget about the basics of internal controls. It is worth stating that many of the lessons learned from those headline cases cited violations of the fundamental tenets of internal control, particularly those pertaining to operational risks. Based on the headlines, it seems that boards of directors, management, and auditors need a remedial course in Internal Controls 101. As corporations grow larger and more diverse, internal controls become more, not less, important to the ability of management and the board to monitor activity across the company.

The basics of internal controls for directors and managers are simple. Directors do not serve full time, so it is important that they establish an annual agenda to focus their attention on the high-risk and

emerging-risk areas while ensuring that there are effective preventive or detective controls over the low-risk areas. Regulatory compliance is one of these risk areas. While boards are organized in various ways, they do have the responsibility to understand the organization of the compliance function and the extent of its effectiveness and to identify the emerging compliance risks. The challenge for compliance officers is to ensure that their staff has the expertise and ongoing training to meet the specific and changing risks of the organization.

Before a company moves into new and higher risk areas, the boards of directors, and management need assurances that they have adherence to the basics of sound governance. Many of the organizations that have seen their reputations tarnished in the past two years have also neglected to consider emerging conflicts of interest when the organization adds new products and lines of business. It is important that if a customer service or control function must be done in an independent, fiduciary, or unbiased manner relative to other activities, appropriate firewalls are in place before the product or activity begins.

Internal controls and compliance are the responsibility of line management. Line managers must determine the acceptable level of risk in their line of business and must assure themselves that the combination of earnings, capital, and internal controls is sufficient to compensate for the risk exposures. Supporting functions such as accounting, internal audit, risk management, credit review, compliance, and legal should independently monitor the control processes to ensure that they are effective and that risks are measured appropriately. The results of these independent reviews should be routinely reported to executive management and boards of directors. Directors should be sufficiently engaged in the process to determine whether these reviews are in fact independent of the operating areas and whether the officers conducting the reviews can speak freely. Directors must demand that management fix problems promptly and provide appropriate evidence to internal audit confirming this.

While we have been focused on midsized and larger organizations, internal controls are also important to smaller organizations. Many failures of community banks are due to breakdowns in internal controls, thus increasing operational risk. In smaller organizations, the segregation of duties and ability to hire expertise for specialized areas, like regulatory compliance, is more difficult. But smaller organizations still must go through the process of assessing risks and controls and ensuring that they are appropriate for the culture and business mix of the organization. A faster-growing financial services company in riskier lines of business will need a stronger, more formalized system of internal controls than a well-established company engaged broadly in traditional financial services.

**Compliance risk management**

To be effective, compliance risk management must be coordinated at various levels within the organization. In any control or oversight function, there are common elements of a successful compliance process that each organization should exhibit. While the diversity, size, and business mix of the organization will affect the specific aspects of an effective process, every financial institution should consider these elements.

*Director and senior management responsibilities*. The board of directors and senior management cannot delegate the responsibility for having an effective system of compliance. Certain portions of the implementation of the compliance process may be conducted by more junior management, but this does not relieve the board and senior management of responsibility for the design and effectiveness of the system.

The board of directors and senior management must set a tone that encourages regulatory compliance. The board should receive periodic reports on the effectiveness of the compliance program and emerging issues. The board should ensure that strategic and product development efforts include an independent view of potential conflicts and new risk exposures. The board should ensure that identified compliance weaknesses are dealt with in a timely fashion, and that the line employees, as well as compliance and internal audit staffs, are trained to keep up with changes in regulations and best practices in internal controls. Most importantly, the board should ensure that the senior compliance officer has independent access to the appropriate board committee, and the senior compliance officer has the stature with senior management to see that appropriate controls are implemented.

While the governance of a bank's risk-management program comes from the top down, a successful program will involve staff at all levels, and in more than one department. In other words, while senior

management bears the ultimate responsibility for successfully managing the compliance risks, management alone cannot contain these risks. This means that the teller who has contact with the customer, the auditor who periodically reviews documents for compliance, the marketing staff who prepare ads and develop new products and the attorney who reviews new forms for compliance all play an integral part in running an effective compliance management program.

*Structure*. The compliance function will vary by the size and complexity of the organization. But the compliance officers should be able to have access to all operational areas. One of the benefits of having an independent compliance function is that it can help identify compliance weaknesses that cross management lines of responsibilities and may not be effectively managed. In larger organizations this may require both business-line and enterprise-wide compliance committees to prioritize resources.

Further, you, as compliance officers, are the independent eyes and ears of the audit and other board committees. As you work throughout the bank, you know which managers and which projects are likely to entail greater weaknesses in compliance. By helping senior management address these risks before exceptions occur, you can help protect the reputation of managers and the bank and increase your credibility. Appropriate reporting to the senior management compliance committee and the audit committee of the board, and timely resolution of findings, will build your credibility, provided that you follow through on their behalf to ensure that managers are taking compliance and internal control issues seriously.

*Scope*. Compliance should have an annual work plan that lays out priorities, monitoring processes, and testing. New or changed regulations have to be evaluated and relevant internal policies appropriately modified. This can entail training for both the line and compliance staff. The frequency and extent of compliance reviews and testing should be consistent with the nature and complexity of the institution's compliance risks. Areas with higher penalties for non-compliance, that have prior findings of deficiencies or where new products or processes are being introduced should receive more attention. Unacceptable exceptions should be reported promptly to appropriate management and, if appropriate, the board of directors. Compliance officers should monitor corrective action plans, and retest to ensure deficiencies are corrected in a timely manner.

As with any risk management function, the management compliance committee and appropriate committee of the board should at least annually review and approve the compliance risk assessment, the scope of the annual plan, and adherence to the compliance plan. While the plan serves as the prioritization of resources, it should be flexible enough to allow appropriate reallocation of resources as unexpected product introductions or compliance testing results require. At the end of each year, the validity of the initial assumptions should be critically assessed and appropriate reallocations of resources scheduled for the new plan year.

*Compliance audits*. The internal audit function should perform independent reviews of the effectiveness of the compliance function. This would include assurance of the quality of information in compliance reports, adequacy of training programs, prompt correction of deficiencies, and implementation of compliance risk management by product managers. The internal auditor can also assess whether sufficient resources are available to meet the changing needs of the organization.

Internal audit should be independent of the compliance function. Auditors lose their independence when they perform management consulting roles for which they later will have to render an opinion. Internal audit has both the ability and the responsibility to look across all of the management silos within the corporation and make sure that the system of internal controls has no gaps. Further, the control framework must be continually reviewed to keep up with corporate strategic initiatives, reorganizations, and process changes. When an auditor becomes part of management, the independent view is lost.

**Sarbanes-Oxley Act**

Now let's turn to Sarbanes-Oxley. At its core, the Sarbanes-Oxley Act is a call to get back to the basics that we have been discussing. **Simply stated, the current status quo for corporate governance is unacceptable and must change.**

This message is applicable to both public and private companies alike and affects everyone within a company.

- The message for boards of directors is: uphold your responsibility for ensuring the effectiveness of the company's overall governance process.
- The message for audit committees is: uphold your responsibility for ensuring that the company's internal and external audit processes are rigorous and effective.
- The message for chief executive and chief financial officers and senior management is: Uphold your responsibility to maintain effective financial reporting and disclosure controls and adhere to high ethical standards. This requires meaningful certifications, codes of ethics, and conduct for insiders that, if violated, will result in fines and criminal penalties, including imprisonment.
- The message for external auditors is: focus your efforts solely on auditing financial statements and leave the add-on services to other consultants.
- The message for internal auditors is: you are uniquely positioned within the company to ensure that its corporate governance, financial reporting and disclosure controls, and risk-management practices are functioning effectively. Although internal auditors are not specifically mentioned in the Sarbanes-Oxley Act, they have within their purview of internal control the responsibility to examine and evaluate all of an entity's systems, processes, operations, functions, and activities.

**What are the challenges for compliance officers in the Sarbanes-Oxley era?**

First, compliance officers must help corporate risk officers and managers reinvigorate the risk assessment, internal controls, and ethical compass of the organization.

Recently, the Fed has been looking at the FDICIA 112 management reports on internal controls for several banks that have had significant breaks in internal controls. From these banks, we have identified several whose FDICIA 112 processes were not effective. A closer look at these situations indicates that managements had essentially put this process on autopilot. Further, the external auditors had not done effective reviews of the basis of management reports.

Before you say, "That could not happen at my company," let me remind you how we started our discussion today. In each of the cases involving banks, management seemed to be content with the loss of vigor in the process and the external auditor was apparently satisfied to simply collect a fee. This is totally unacceptable. Further, as the organization evolves by offering new products, changing processes, outsourcing services, complying with new regulations, or growing through mergers, the controls need to be modified to reflect the changes in risks. In some cases, the controls failed with respect to newer risk exposures that were not identified, or growth put strains on existing control processes that were not suitable for a larger organization.

Don't assume that what was acceptable in the past is good enough for the future. Remember that there is a tendency for an organization to go on autopilot if the compliance officer is not vigilant. You should view this as an opportunity to convince the board and management to adopt a rigorous self-assessment process for compliance controls. Further, use this as an opportunity to improve your own quality assurance process. Are you surprised by exceptions? Do you find your staff coming to different findings for compliance reviews that have similar fact patterns? Are you harder on some managers in your findings, and "trust" others to improve without citing the weaknesses? When you do not have a consistent quality for the work of the compliance function you send mixed messages to employees and officers. Further, you weaken your credibility. And more importantly in the current environment, you are not part of the process to strengthen corporate governance.

Now, certainly, we must know which way the ethical compass of the organization is pointing. Are the product designs, marketing practices, and disclosures communicating a solid image of trust and integrity that your organization is targeting?

**Conclusion**

My objective today was to exhort you to take a stand and make a difference for the better in the corporate governance of your company. You should help lead the dialogue on corporate governance. Although I recognize that some of you are compliance officers of companies that are not subject to

Sarbanes-Oxley, I believe the act is a wake-up call more generally for everyone who is part of designing and testing a system of internal controls.

The events of the past two years demonstrate how quickly a corporation's reputation can be tainted by accusations of inappropriate activities or lack of attention to regulations. Success in banking still is heavily dependent on winning and keeping the trust of customers, employees, and communities. When corporate reputations are tainted, it can take a considerable time to rebuild customer and community relationships.